On the $\mathbb{F}_2$-linear relations of Mersenne Twister pseudorandom number generators

Shin Harase[a,*]

[a] *Graduate School of Innovation Management, Tokyo Institute of Technology, W9-115, 2-12-1 Ookayama, Meguro-ku,Tokyo, 152-8550, Japan.*

Abstract

Sequence generators obtained by linear recursions over the two-element field $\mathbb{F}_2$ are widely used as pseudorandom number generators. For example, the Mersenne Twister MT19937 is one of the most successful applications. An advantage of such generators is that we can assess them by using theoretical criteria, such as the dimension of equidistribution with v-bit accuracy. To compute these dimensions, several lattice reduction methods have been proposed.

In this paper, we focus on the relationship between points in the Couture–L'Ecuyer dual lattices and $\mathbb{F}_2$-linear relations on the most significant v bits of output sequences, and consider a new figure of merit N_v based on the minimum weight of $\mathbb{F}_2$-linear relations whose degrees are minimal for v. Next, we apply the figure of merit to the Mersenne Twister MT19937. Our experimental results show that MT19937 has low-weight $\mathbb{F}_2$-linear relations in dimensions higher than 623, and that some output vectors with specific lags are rejected or have small p-values in the birthday spacings tests. We also report that some variants of Mersenne Twister, such as WELL generators, are significantly improved from the perspective of N_v.

Keywords: Random number generation, Lattice structure, Statistical test
2010 MSC: 65C10, 11K45

*Corresponding author
Email address: harase@craft.titech.ac.jp (Shin Harase)

1. Introduction

The *Mersenne Twister* MT19937 is a pseudorandom number generator developed by Matsumoto and Nishimura [26]. This generator has the following advantages: (i) Its generation speed is very fast; (ii) it has a large period of $2^{19937}-1$; (iii) it has high-dimensional equidistribution property (i.e., 623-dimensionally equidistributed). Thus, MT19937 is currently one of the most widely used pseudorandom number generators in Monte Carlo simulations. For example, it is the default generator for a recent version of R (see [35]), it is presented in the GNU Scientific Library, and it is implemented in a large number of programming languages.

The algorithm of the Mersenne Twister is based on the following linear recurrence over the two-element field $\mathbb{F}_2 := \{0, 1\}$:

$$\mathbf{m}_i := \mathbf{m}_{i+n_2-n_1} \oplus \tilde{\mathbf{A}}(\mathbf{m}_{i-n_1}^{w-r} | \mathbf{m}_{i-n_1+1}^{r}) \quad (i = 0, 1, 2, \ldots), \tag{1}$$

where $\mathbf{m}_i \in \mathbb{F}_2^w$ is a w-bit vector (w indicates the word size of machines), n_1 is the degree of recurrence, n_2 is an integer with $1 \le n_2 \le n_1$, $\oplus$ denotes the component-wise addition modulo 2 (i.e., bitwise exclusive-or in the computer terminology), $\tilde{\mathbf{A}}$ is a suitable $w \times w$ matrix with elements in $\mathbb{F}_2$, r is an integer with $0 \le r \le w-1$, $\mathbf{m}_{i-n_1}^{w-r}$ is the upper $w-r$ coordinates of $\mathbf{m}_{i-n_1}$, $\mathbf{m}_{i-n_1+1}^{r}$ is the lower r coordinates of $\mathbf{m}_{i-n_1+1}$, and $(\mathbf{m}_{i-n_1}^{w-r} | \mathbf{m}_{i-n_1+1}^{r}) \in \mathbb{F}_2^w$ denotes a vector that is the concatenation of $\mathbf{m}_{i-n_1}^{w-r}$ and $\mathbf{m}_{i-n_1+1}^{r}$. We set $\mathbf{m}_{-1}, \mathbf{m}_{-2}, \ldots, \mathbf{m}_{i-n_1}$ as initial seeds. Furthermore, in order to improve the high-dimensional equidistribution property, we execute a linear output transformation by multiplying a suitable $w \times w$ invertible matrix $\mathbf{T}$:

$$\mathbf{y}_i := \mathbf{T}\mathbf{m}_i, \tag{2}$$

which is said to be the *tempering* proposed by Matsumoto and Kurita [24]. Throughout this paper, we identify a w-dimensional vector $\mathbf{y}_i = {}^t(y_{i,0}, \ldots, y_{i,w-1})$ with an unsigned w-bit binary integer (^{t} denotes the *transpose* of a vector), and a binary expansion $u_i := \sum_{l=1}^{w} y_{i,l-1} 2^{-l}$ as a real number in the interval $[0, 1)$. The output sequence $\{u_i\}$ is supposed to imitate independent random variables that are uniformly distributed over $[0, 1)$. The Mersenne Twister MT19937 has the parameter set $(w, n_1, n_2, r) = (32, 624, 397, 31)$ and selected matrices $\tilde{\mathbf{A}}$ and $\mathbf{T}$, which can be computed rapidly. As a result, we have a maximal period of $2^{19937}-1$ (i.e., $2^{n_1 w - r} - 1$), which is a *Mersenne prime*.

Here, the following two quality criteria for linear pseudorandom number generators over $\mathbb{F}_2$ (so-called $\mathbb{F}_2$-*linear generators*) are well-known: (i) the

dimension of equidistribution with v-bit accuracy $k(v)$ for each v ($1 \le v \le w$) and (ii) the number N_1 of nonzero terms in a characteristic polynomial. From this perspective, MT19937 was considered to be much superior to all other classical generators when it appeared approximately 15 years ago, and it has since become widely used as the most innovative generator.

However, it may not be sufficient for assessing the quality of generators using only the above two criteria. In this paper, we develop a new figure of merit N_v based on the minimum number of nonzero terms of $\mathbb{F}_2$-linear relations whose degrees are minimal for the most significant v bits given. The value N_v can be considered as a quality criteria in dimensions higher than $k(v)$ and as a multi-dimensional generalization of N_1. We assess the Mersenne Twister MT19937 and its variants in terms of N_v's, and show that N_v's of MT19937 are small, relative to the WELL generators [34]. We also report that MT19937 has some deviations in the birthday spacings test [22, 11, 14, 15] for non-successive output values, which are probably because of the existence of low-weight $\mathbb{F}_2$-linear relations.

The rest of this paper is organized as follows. In Section 2, we recall a framework of $\mathbb{F}_2$-linear generators. In Section 3, we explain the terminologies of $k(v)$ and N_1. In Section 4, to use later sections, we briefly survey the Couture–L'Eucyuer dual lattice method [2] for computing $k(v)$. In Section 5, we show the relationship between $\mathbb{F}_2$-linear relations and points in the Couture–L'Ecuyer dual lattices, define a new figure of merit N_v, and give an algorithm for computing N_v using Gray codes. In Section 6, we analyze the Mersenne Twister MT19937 in terms of both N_v's and $\mathbb{F}_2$-linear relations. In Section 7, we report some deviations of MT19937 in birthday spacings tests with selected lags. Section 8 is devoted to the analysis of other $\mathbb{F}_2$-linear generators, such as the WELL generators. We also introduce a new tempering parameter of MT19937 in order to optimize $k(v)$ as an improvement of the author's previous work [7]. Our conclusions are presented in Section 9.

2. $\mathbb{F}_2$-linear generators

Mersenne Twister generators belong to a general class of pseudorandom number generators based on the following matrix recurrences over $\mathbb{F}_2$:

$$\mathbf{x}_i := \mathbf{A}\mathbf{x}_{i-1}, \tag{3}$$

$$\mathbf{y}_i := \mathbf{B}\mathbf{x}_i, \tag{4}$$

$$u_i \;:=\; \sum_{l=1}^{w} y_{i,l-1}2^{-l} = 0.y_{i,0}y_{i,1}\cdots y_{i,w-1}, \tag{5}$$

where $\mathbf{x}_i = {}^t(x_{i,0},\ldots,x_{i,p-1}) \in \mathbb{F}_2^p$ is the p-bit *state vector* at step i; $\mathbf{y}_i = {}^t(y_{i,0},\ldots,y_{i,w-1}) \in \mathbb{F}^w$ is the w-bit *output vector* at step i; p and w are positive integers, $\mathbf{A}$ is a $p\times p$ *transition matrix* with elements in $\mathbb{F}_2$, and $\mathbf{B}$ is a $w\times p$ *output transformation matrix* with elements in $\mathbb{F}_2$. The real number $u_i \in [0,1)$ is the *output* at step i. All operations in (3) and (4) are performed in $\mathbb{F}_2$, i.e., modulo 2. This framework is said to be the $\mathbb{F}_2$-*linear generator*. Refer to [13, 28] for details.

Let $P(z) := \det(\mathbf{I}z - \mathbf{A})$ be the *characteristic polynomial* of $\mathbf{A}$. The recurrence (3) has the period length $2^p - 1$ (its maximal possible value) if and only if $P(z)$ is a primitive polynomial modulo 2 (see [30, 11]). When this maximum is reached, we say that the $\mathbb{F}_2$-linear generator has the *maximal period*. For simplicity, we assume the maximal-period condition throughout this paper.

From Section 2.3.5 in [33], the Mersenne Twister (1) fits the above framework by the transition matrix

$$\mathbf{A} = \begin{pmatrix} & & & \mathbf{I}_w & & & \mathbf{S} \\ \mathbf{I}_w & & & & & & \\ & \mathbf{I}_w & & & & & \\ & & \ddots & & & & \\ & & & & \ddots & & \\ & & & & & \mathbf{I}_{w-r} & \end{pmatrix}, \; \mathbf{S} = \tilde{\mathbf{A}} \begin{pmatrix} \mathbf{0} & \mathbf{I}_{w-r} \\ \mathbf{I}_r & \mathbf{0} \end{pmatrix}, \tag{6}$$

where $\mathbf{I}_w, \mathbf{I}_r, \mathbf{I}_{w-r}$ are the identity matrices of size $w, r, w-r$, respectively, and $\mathbf{x}_i = {}^t({}^t\mathbf{m}_i, {}^t\mathbf{m}_{i-1}\ldots, {}^t\mathbf{m}_{i-n_1+2}, {}^t\mathbf{m}^{w-r}_{i-n_1+1})$ in (3), so that $p = n_1 w - r$. (Note that MT19937 has $p = 19937$.) For the tempering in (2), the matrix $\mathbf{B}$ is the representation matrix of the following transformation:

$$\mathbf{z} \;\leftarrow\; \mathrm{trunc}_w(\mathbf{x}_i) \tag{7}$$

$$\mathbf{y}_i \;\leftarrow\; \mathbf{T}\mathbf{z} \tag{8}$$

where "$\leftarrow$" represents the assignment statement, and $\mathrm{trunc}_w(\mathbf{x}_i)$ denotes the vector ${}^t(x_{i,0},\ldots,x_{i,w-1})$, which is formed by leading w coordinates of $\mathbf{x}_i$,

3. Quality criteria

Following [13], we recall figures of merit for $\mathbb{F}_2$-linear generators.

A primary requirement for long-period $\mathbb{F}_2$-linear pseudorandom number generators is that k-dimensional vectors $(u_i, u_{i+1}, \ldots, u_{i+k-1})$ are uniformly distributed over the unit hypercube $[0,1)^k$ for large k. From this viewpoint, we often use the terminology of the *dimension of equidistribution with v-bit accuracy*. Let Ψ_k be the multiset of k-dimensional vectors, from all possible initial states $\mathbf{x}_0$:

$$\Psi_k := \{(u_0, \ldots, u_{k-1}) \mid \mathbf{x}_0 \in \mathbb{F}_2^p\} \subset [0,1)^k. \tag{9}$$

Let us equate each axis $[0,1)$ into 2^v pieces. Then, $[0,1)^k$ is divided into 2^{kv} cubic cells of equal size. The generator is said to be *k-dimensionally equidistributed with v-bit accuracy* if each cell contains exactly the same number of points of Ψ_k, i.e., 2^{p-kv} points. The largest value of k with this property is called the *dimension of equidistribution with v-bit accuracy*, denoted by $k(v)$. As a criterion of uniformity, larger $k(v)$ for each $1 \le v \le w$ is desirable (see [39]). We have a trivial upper bound $k(v) \le \lfloor p/v \rfloor$. The gap $d(v) := \lfloor p/v \rfloor - k(v)$ is called the *dimension defect* at v, and their sum $\Delta := \sum_{v=1}^{w} (\lfloor p/v \rfloor - k(v))$ is called the *total dimension defect*. If $\Delta = 0$, the generator is said to be *maximally equidistributed*. Note that MT19937 has $\Delta = 6750$, and $k(v)$ does not always attain the upper bound for each $1 \le v \le w$.

As a secondary requirement, we may consider whether the number N_1 of nonzero coefficients for a given characteristic polynomial $P(z)$ is greater (see [1, 41]). Ideally, we desire that N_1 is close to a half degree of $P(z)$ (i.e., $p/2$). For example, according to [19, 25, 27], generators for which $P(z)$ is a trinomial or a pentanomial fail statistical tests, so we should avoid such generators. MT19937 has $N_1 = 135$ nonzero coefficients in $P(z)$, whose number is much greater than three or five. Panneton, L'Ecuyer, and Matsumoto [34] noted that N_1 of MT19937 is still smaller than $p/2$ and MT19937 has a long-lasting impact for a bad initial state (e.g., one that contains only a few bits set to 1), when compared to their WELL generators, whose N_1's are almost $p/2$. Thus, N_1 (or N_1/p) is also used as a figure of merit for $\mathbb{F}_2$-linear generators.

The above figures of merit are commonly used. To investigate theoretical properties in more detail, we may consider a new criterion from another perspective.

4. Lattice structures

We briefly recall a lattice method for computing $k(v)$ in terms of the dual lattices [2, 13]. Let K denote the formal power series field $K := \mathbb{F}_2((z^{-1})) = \{\sum_{i=i_0}^{\infty} a_i z^{-i} \mid a_i \in \mathbb{F}_2, i_0 \in \mathbb{Z}\}$. For $a(z) = \sum_{i=i_0}^{\infty} a_i z^{-i} \in K$, we define a standard norm by

$$|a(z)| := \begin{cases} \max\{-i \in \mathbb{Z} \mid a_i \neq 0\} & \text{if } a(z) \neq 0, \\ -\infty & \text{if } a(z) = 0. \end{cases}$$

For a vector $\mathbf{a}(z) = {}^t(a_0(z), a_1(z), \ldots, a_{v-1}(z)) \in K^v$, we define its *norm* (or its *length*) by $||\mathbf{a}(z)|| := \max_{1 \le l \le v} |a_{l-1}(z)|$.

A subset $L \subset K^v$ is said to be an $\mathbb{F}_2[z]$-*lattice* if there exists a K-linear basis $\{\mathbf{v}_1(z), \mathbf{v}_2(z), \ldots, \mathbf{v}_v(z)\}$ of K^v such that L is their span over $\mathbb{F}_2[t]$, i.e.,

$$L = \langle \mathbf{v}_1(z), \mathbf{v}_2(z), \ldots, \mathbf{v}_v(z) \rangle_{\mathbb{F}_2[t]}.$$

Such a set of vectors is called a *basis* of L. We recall the following theorem, which will be used later:

Theorem 1 ([20, 21]). *Let $\mathbf{v}_1(z), \ldots, \mathbf{v}_v(z)$ be the points in an $\mathbb{F}_2[z]$-lattice $L \subset K^v$ with the following properties:*

1. *$\mathbf{v}_1(z)$ is a shortest nonzero vector in L;*
2. *for $l = 2, \ldots, v$, $\mathbf{v}_l(z)$ is a shortest vector among the set of vectors $\mathbf{v}(z)$ in L such that $\mathbf{v}_1(z), \ldots, \mathbf{v}_{l-1}(z), \mathbf{v}(z)$ are linearly independent over K.*

Then $\mathbf{v}_1(z), \ldots, \mathbf{v}_v(z)$ form a basis of L.

In the above theorem, such a basis is said to be a *reduced basis* of L. It is not unique, but the numbers $\nu_l := ||\mathbf{v}_l(z)||$ $(l = 1, \ldots, v)$ are uniquely determined by a given lattice L, and $\nu_1, \ldots, \nu_v$ are called the *successive minima* of L.

Here, we consider an $\mathbb{F}_2$-linear generator. For a given nonzero initial state $\mathbf{x}_0 \in \mathbb{F}_2^p$, we define the following formal power series $G_{l-1}(z)$ of lth bits of the integer output (i.e., $y_{0,l-1}, y_{1,l-1}, y_{2,l-1}, \cdots$):

$$G_{l-1}(z) := \sum_{i=0}^{\infty} y_{i,l-1} z^{-i-1} = y_{0,l-1} z^{-1} + y_{1,l-1} z^{-2} + y_{2,l-1} z^{-3} + \cdots \in \mathbb{F}_2((z^{-1})).$$

Note that $G_{l-1}(z)$ has a rational form $G_{l-1}(z) = h_{l-1}(t)/P(z)$, where $h_{l-1}(z) \in \mathbb{F}_2[z]$ and $\deg h_{l-1}(z) < \deg P(z)$. If $P(z)$ is irreducible, let $h_0^{-1}(z)$ be a

polynomial that is a multiplicative inverse to $h_0(z)$ modulo $P(z)$. We set $\bar{h}_{l-1}(z) := h_0^{-1}(z)h_{l-1}(z) \bmod P(z)$ $(2 \le l \le v)$. We consider the following vectors

$$\begin{aligned}
\mathbf{w}_1(z) &:= {}^t(P(z), 0, 0, \ldots, 0), \\
\mathbf{w}_2(z) &:= {}^t(-\bar{h}_1(z), 1, 0, \ldots, 0), \\
\mathbf{w}_3(z) &:= {}^t(-\bar{h}_2(z), 0, 1, \ldots, 0), \\
&\vdots \\
\mathbf{w}_v(z) &:= {}^t(-\bar{h}_{v-1}(z), 0, 0, \ldots, 1),
\end{aligned}$$

and construct an $\mathbb{F}_2[z]$-lattice $\mathcal{L}_v^* := \langle \mathbf{w}_1(z), \ldots, \mathbf{w}_v(z) \rangle_{\mathbb{F}_2[z]} \subset \mathbb{F}_2^v[z]$, which is said to be the Couture–L'Ecuyer *dual lattice* [2].

Theorem 2 ([2]). *We consider an $\mathbb{F}_2$-linear generator started from a nonzero initial state vector. Assume that the characteristic polynomial $P(z)$ of $\mathbf{A}$ is primitive. Then, $k(v) = \nu_1^*$, where ν_1^* is the first successive minimum of $\mathcal{L}_v^*$.*

We can obtain a reduced basis by using some polynomial-time lattice basis reduction algorithms (e.g., [6, 18, 37, 29]).

Remark 1. Recently, the author, Matsumoto, and Saito [10] proposed the *SIS* method for computing $k(v)$, which is faster than the Couture–L'Ecuyer dual lattice one, and the author [8] proposed the PIS method as an improvement over SIS. The new methods use the lattice points in the original lattices [3, 38] (not the dual lattices $\mathcal{L}_v^*$). As a classical result, it is also possible to compute $k(v)$ by using linear algebra [5]. The aim of this paper is to extract other information from $\mathcal{L}_v^*$. This is why we consider the Couture–L'Ecuyer dual lattice method.

5. A new figure of merit for $\mathbb{F}_2$-linear generators

Usually, when we assess an $\mathbb{F}_2$-linear generator, we only see the length of a shortest vector (i.e., $k(v)$) as the first filter, and abandon the other information. In this section, we focus on the polynomial elements of vectors in $\mathcal{L}_v^*$, and develop a new figure of merit N_v as a quality criterion in dimensions that are higher than $k(v)$ and as a multi-dimensional generalization of N_1.

First, we arrange the relationship between $\mathbb{F}_2$-linear relations appeared on the most significant v bits and points in $\mathcal{L}_v^*$. The following proposition is obtained by a modification of Lemma 4.40 in [30].

Proposition 3. *There exists an $\mathbb{F}_2$-linear relation*

$$\sum_{l=1}^{v}\sum_{j=0}^{k-1} w_{j,l-1}y_{i+j,l-1} = 0 \text{ for all } i \geq 0, \tag{10}$$

if and only if ${}^t(w_0(z)), \ldots, w_{v-1}(z)) \in \mathcal{L}_v^*$, *where* $w_{l-1}(z) := \sum_{j=0}^{k-1} w_{j,l-1}z^j \in \mathbb{F}_2[z]$.

Proof. We consider a linear combination

$$G_0(z)w_0(z) + \cdots + G_{l-1}(z)w_{l-1}(z). \tag{11}$$

For $i \geq 0$, the coefficient of z^{-i-1} in (11) is $\sum_{l=1}^{v}\sum_{j=0}^{k-1} w_{j,l-1}y_{i+j,l-1}$, so that the coefficients of the negative power are all zero if and only if (10) holds. Then, (11) is a polynomial. On the other hand, (11) is also described as $(h_0(z)w_0(z) + \cdots + h_{v-1}(z)w_{v-1}(z))/P(z)$. Thus, (10) is equivalent to

$$h_0(z)w_0(z) + \cdots + h_{v-1}(z)w_{v-1}(z) \equiv 0 \bmod P(z). \tag{12}$$

Here, we assume (10). By multiplying (12) by $h_0^{-1}(z)$, we have $w_0(z) \equiv -\bar{h}_1(z)w_1(z) - \cdots - \bar{h}_{v-1}(z)w_{v-1}(z) \bmod P(z)$. In (12), each of polynomial solutions ${}^t(w_0(z), \ldots, w_{v-1}(z))$ is written as $-a(z)\mathbf{w}_1(z) + h_1(z)\mathbf{w}_2(z) + \cdots + h_{v-1}(z)\mathbf{w}_v(z) = {}^t(-a(z)P(z) - \bar{h}_1(z)w_1(z) - \cdots - \bar{h}_{v-1}(z)w_{v-1}(z), w_1(z), \ldots, w_{v-1}(z))$ for a suitable $a(z) \in \mathbb{F}_2[z]$. Hence, ${}^t(w_0(z), \ldots, w_{v-1}(z)) \in \mathcal{L}_v^*$.

Conversely, it is easy to see that all of $\mathbb{F}_2[z]$-linear combinations of $\mathbf{w}_1(z), \ldots, \mathbf{w}_v(z)$ satisfy (12), because $\mathbf{w}_1(z), \ldots, \mathbf{w}_{v-1}(z)$ are solutions in (12), respectively. Thus, the proposition follows.

Using the above proposition, from vectors of $\mathcal{L}_v^*$, we obtain information on $\mathbb{F}_2$-linear relations in dimensions that are higher than $k(v)$. In particular, a nonzero shortest vector of $\mathcal{L}_v^*$ corresponds to a non-trivial $\mathbb{F}_2$-linear relation

$$\sum_{l=1}^{v}\sum_{j=0}^{k(v)} w_{j,l-1}y_{i+j,l-1} = 0 \text{ for all } i \geq 0, \tag{13}$$

whose degree is minimal for the most significant v bits given. We call (13) a *minimal $\mathbb{F}_2$-linear relation with v-bit accuracy*. In general, such a minimal $\mathbb{F}_2$-linear relation is not unique, because a shortest vector is not unique. Furthermore, we have no non-trivial $\mathbb{F}_2$-linear relation $\sum_{l=1}^{v}\sum_{j=0}^{k} w_{j,l-1}y_{i+j,l-1} = 0$

for $k < k(v)$. All of the minimal $\mathbb{F}_2$-linear relations with v-bit accuracy are included in all the vectors whose dimensions are higher than $k(v)$, so that the $(k(v)+1)$-dimensional case appears to be the most important.

Here, to assess the $\mathbb{F}_2$-linear generators, let us consider whether or not the minimal $\mathbb{F}_2$-linear relations have simple regularity. The simplest way of checking this is to enumerate the number of nonzero coefficients $w_{j,l-1}$ in (13). We call this the *weight*. When there exist low-weight $\mathbb{F}_2$-linear relations, the generator may have risks in some situations (see Remark 2). Therefore, we define the *minimum weight* N_v by the lowest weight for all the minimal $\mathbb{F}_2$-linear relations with v-bit accuracy in (13), and propose N_v as a new figure of merit for $\mathbb{F}_2$-linear generators. When $v = 1$, the minimal $\mathbb{F}_2$-linear relation (13) coincides with a characteristic polynomial $P(z)$, so that N_v equals the number N_1 of nonzero coefficients of $P(z)$. Hence, we can interpret N_v as a multi-dimensional generalization of N_1.

For practical use, we give an algorithm for computing N_v as follows. Let $\{\tilde{\mathbf{w}}_1(z), \ldots, \tilde{\mathbf{w}}_v(z)\}$ be a reduced basis of $\mathcal{L}_v^*$. From the uniqueness of the successive minima, we have an integer $v' \in \{1, \ldots, v\}$ such that $||\tilde{\mathbf{w}}_1(z)|| = \cdots = ||\tilde{\mathbf{w}}_{v'}(z)|| < ||\tilde{\mathbf{w}}_{v'+1}(z)|| \le \cdots \le ||\tilde{\mathbf{w}}_v(z)||$. Then, all the shortest vectors are described by

$$\{c_1\tilde{\mathbf{w}}_1(z) + \ldots + c_{v'}\tilde{\mathbf{w}}_{v'}(z) \mid {}^t(c_1, \ldots, c_{v'}) \in \mathbb{F}_2^{v'} \setminus {}^t(0, \ldots, 0)\}, \tag{14}$$

and they correspond to all the minimal $\mathbb{F}_2$-linear relations with v-bit accuracy. The number of the shortest vectors is $2^{v'} - 1$. Here, if we give coefficients $c_1, \ldots, c_{v'}$ by v'-bit Gray code order, it is possible to obtain another shortest vector by executing the addition only once. In addition, if v' is small and p is not too large (e.g., $v' \le 32$ and $p \le 19937$), we can compute the minimum weight N_v within a practical time period.

Remark 2. We mention a strong relationship between our figure of merit N_v and the *weight discrepancy test* proposed by Matsumoto and Nishimura [27]. For simplicity, consider k successive output values with v-bit accuracy, where $k > k(v)$, and let Φ be the map from the state vectors to $m := v \times k$ bits in the outputs:

$$\Phi : \mathbb{F}_2^p \to \mathbb{F}_2^m, \quad \mathbf{x}_0 \mapsto (\mathrm{trunc}_v(\mathbf{y}_0), \mathrm{trunc}_v(\mathbf{y}_1), \ldots, \mathrm{trunc}_v(\mathbf{y}_{k-1})). \tag{15}$$

The map Φ is $\mathbb{F}_2$-linear, so that the image $C \subset \mathbb{F}_2^m$ is a linear subspace. In coding theory, C is said to be a *linear code*. The *dual code* $C^\perp$ of C is defined

by

$$C^{\perp} := \{\mathbf{c}' \in \mathbb{F}_2^m \mid \langle \mathbf{c}', \mathbf{c} \rangle = 0 \text{ for all } \mathbf{c} \in C\},$$

where $\langle \mathbf{c}', \mathbf{c} \rangle = \sum_{i=1}^{m} c'_i c_i$ is an inner product for $\mathbf{c}' = {}^t(c'_1, \ldots, c'_m) \in \mathbb{F}_2^m$ and $\mathbf{c} = {}^t(c_1, \ldots, c_m) \in \mathbb{F}_2^m$. Note that $C^{\perp}$ contains the set of $\mathbb{F}_2$-linear relations on $m = k \times v$ bits (see [27]).

The weight discrepancy test is a theoretical test for estimating the deviation of the number of 1's on $m = v \times s$ bits in (15) from the binomial distribution. Matsumoto and Nishimura [27] gave a formula for computing a risky sample size from a weight enumerator polynomial of C, which is computed via a weight enumerator polynomial of $C^{\perp}$ with k being slightly greater than $k(v)$, and via inversion by the MacWilliams identity. Their paper implies that if the minimum weight of vectors of $C^{\perp}$ is more than 15 or 20, a given generator is safe, but if the weights are too low (e.g., ≤ 6), there may be a possibility of detecting deviations. In fact, we can identify $C^{\perp}$ with a set of all the vectors whose lengths are shorter than k, so that N_v coincides with the minimum weight of vectors in $C^{\perp}$ in the case where $k = k(v) + 1$. Thus, when N_v is small, a given generator may have some risks.

A drawback of N_v is that we have to execute exhaustive searches, such as (14) because the weight enumeration (or finding the minimum weight N_v) is NP-hard [40]. However, from the viewpoint of speed and memory efficiency, the use of the Couture–L'Ecuyer dual lattice method appears to be much superior to the use of the Gaussian elimination on a $p \times m$ matrix in [27] when we construct a basis of $C^{\perp}$ (as an $\mathbb{F}_2$-linear vector space) for a large p.

6. $\mathbb{F}_2$-linear relations of Mersenne Twister MT19937

In this section, we numerically analyze 32-bit Mersenne Twister MT19937 (i.e., $w = 32$) in terms of the method in Section 5. Tables 1 and 2 list the successive minima $\nu_1^*, \nu_2^*, \ldots, \nu_v^*$ of $\mathcal{L}_v^*$, the dimension defect $d(v)$ at v, and our new figure of merit N_v for each $1 \leq v \leq 32$. From Theorem 2, note that $\nu_1 = k(v)$. As a result, N_v's for lower bits are small.

To conduct statistical tests in the next section, we introduce the minimal $\mathbb{F}_2$-linear relations with 21-bit and 12-bit accuracy, for example. First, we analyze the minimal $\mathbb{F}_2$-linear relations with 21-bit accuracy. By checking all the nonzero shortest vectors in $\mathcal{L}_{21}^*$, we obtain the following low-weight $\mathbb{F}_2$-linear relations: the six-term linear relation

$$y_{i,1} + y_{i,16} + y_{i+396,2} + y_{i+396,17} + y_{i+623,2} + y_{i+623,17} = 0,$$

Table 1: The successive minima, $d(v)$, and N_v of MT19937.

	$\mathcal{L}_1^*$	$\mathcal{L}_2^*$	$\mathcal{L}_3^*$	$\mathcal{L}_4^*$	$\mathcal{L}_5^*$	$\mathcal{L}_6^*$	$\mathcal{L}_7^*$	$\mathcal{L}_8^*$	$\mathcal{L}_9^*$	$\mathcal{L}_{10}^*$	$\mathcal{L}_{11}^*$	$\mathcal{L}_{12}^*$	$\mathcal{L}_{13}^*$	$\mathcal{L}_{14}^*$	$\mathcal{L}_{15}^*$	$\mathcal{L}_{16}^*$
ν_1^*	19937	9968	6240	4984	3738	3115	2493	2492	1869	1869	1248	1246	1246	1246	1246	1246
ν_2^*		9969	6848	4984	3738	3115	2493	2492	1869	1869	1868	1246	1246	1246	1246	1246
ν_3^*			6849	4984	3738	3115	2493	2492	1870	1869	1869	1247	1246	1246	1246	1246
ν_4^*				4985	3739	3116	3114	2492	1870	1869	1869	1247	1246	1246	1246	1246
ν_5^*					4984	3738	3114	2492	2491	1869	1869	1868	1246	1246	1246	1246
ν_6^*						3738	3115	2492	2492	1869	1869	1869	1247	1246	1246	1246
ν_7^*							3115	2492	2492	1870	1869	1869	1247	1246	1246	1246
ν_8^*								2493	2492	1870	1869	1869	1868	1246	1246	1246
ν_9^*									2492	2491	1869	1869	1869	1247	1246	1246
ν_{10}^*										2492	1869	1869	1869	1247	1246	1246
ν_{11}^*											1869	1869	1869	1868	1246	1246
ν_{12}^*												1869	1869	1869	1247	1246
ν_{13}^*													1869	1869	1247	1246
ν_{14}^*														1869	1868	1246
ν_{15}^*															1869	1246
ν_{16}^*																1247
$d(v)$	0	0	405	0	249	207	355	0	346	124	564	415	287	178	83	0
N_v	135	10020	393	128	44	57	38	15	10	10	40	5	5	5	5	5

the seven-term linear relations

$$
\begin{aligned}
&y_{i,7} + y_{i,14} + y_{i,15} + y_{i+396,8} + + y_{i+396,16} + y_{i+623,8} + y_{i+623,16} = 0,\\
&y_{i,3} + y_{i+396,1} + + y_{i+396,4} + y_{i+396,19} + y_{i+623,1} + y_{i+623,4} + y_{i+623,19} = 0,\\
&y_{i,2} + y_{i,9} + y_{i,10} + y_{i,17} + y_{i,20} + y_{i+396,11} + y_{i+623,11} = 0,
\end{aligned}
$$

and so on. In particular, all of the minimal $\mathbb{F}_2$-linear relations concentrate on the three non-successive output values $\{\mathbf{y}_i, \mathbf{y}_{i+396}, \mathbf{y}_{i+623}\}$.

In addition to the above, we analyze the minimal $\mathbb{F}_2$-linear relations with 12-bit accuracy. In this case, we have three minimal $\mathbb{F}_2$-linear relations, i.e., the five-term linear relation

$$
y_{i,2} + y_{i+792,4} + y_{i+792,11} + y_{i+1246,4} + y_{i+1246,11} = 0, \tag{16}
$$

and the 18-term and the 19-term linear relations. They appear only on the five non-successive output values $\{\mathbf{y}_i, \mathbf{y}_{i+396}, \mathbf{y}_{i+623}, \mathbf{y}_{i+792}, \mathbf{y}_{i+1246}\}$.

Consequently, we aim to determine whether there are any observable deviations for such non-successive output values.

Remark 3. Niederreiter [31, 32] proposed the *multiple-recursive matrix method* as a general class of pseudorandom number generators. In this framework, we can describe Mersenne Twisters in (1) and (2) by the following matrix linear recurrence:

$$
\mathbf{y}_i = \mathbf{y}_{i+n_2-n_1} + \mathbf{T}\tilde{\mathbf{A}} \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_r \end{pmatrix} \mathbf{T}^{-1}\mathbf{y}_{i+1-n_1} + \mathbf{T}\tilde{\mathbf{A}} \begin{pmatrix} \mathbf{I}_{w-r} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \mathbf{T}^{-1}\mathbf{y}_{i-n_1}.
$$

Table 2: The successive minima, $d(v)$, and N_v of MT19937 (continued).

	$\mathcal{L}_{17}^*$	$\mathcal{L}_{18}^*$	$\mathcal{L}_{19}^*$	$\mathcal{L}_{20}^*$	$\mathcal{L}_{21}^*$	$\mathcal{L}_{22}^*$	$\mathcal{L}_{23}^*$	$\mathcal{L}_{24}^*$	$\mathcal{L}_{25}^*$	$\mathcal{L}_{26}^*$	$\mathcal{L}_{27}^*$	$\mathcal{L}_{28}^*$	$\mathcal{L}_{29}^*$	$\mathcal{L}_{30}^*$	$\mathcal{L}_{31}^*$	$\mathcal{L}_{32}^*$
ν_1^*	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_2^*	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_3^*	1246	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_4^*	1246	623	623	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_5^*	1246	1246	623	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_6^*	1246	1246	624	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_7^*	1246	1246	1246	623	623	623	623	623	623	623	623	623	623	623	623	623
ν_8^*	1246	1246	1246	624	623	623	623	623	623	623	623	623	623	623	623	623
ν_9^*	1246	1246	1246	1246	623	623	623	623	623	623	623	623	623	623	623	623
ν_{10}^*	1246	1246	1246	1246	624	623	623	623	623	623	623	623	623	623	623	623
ν_{11}^*	1246	1246	1246	1246	1246	623	623	623	623	623	623	623	623	623	623	623
ν_{12}^*	1246	1246	1246	1246	1246	624	623	623	623	623	623	623	623	623	623	623
ν_{13}^*	1246	1246	1246	1246	1246	1246	623	623	623	623	623	623	623	623	623	623
ν_{14}^*	1246	1246	1246	1246	1246	1246	624	623	623	623	623	623	623	623	623	623
ν_{15}^*	1246	1246	1246	1246	1246	1246	1246	623	623	623	623	623	623	623	623	623
ν_{16}^*	1246	1246	1246	1246	1246	1246	1246	624	623	623	623	623	623	623	623	623
ν_{17}^*	1247	1246	1246	1246	1246	1246	1246	1246	623	623	623	623	623	623	623	623
ν_{18}^*		1247	1246	1246	1246	1246	1246	1246	624	623	623	623	623	623	623	623
ν_{19}^*			1246	1246	1246	1246	1246	1246	1246	623	623	623	623	623	623	623
ν_{20}^*				1246	1246	1246	1246	1246	1246	624	623	623	623	623	623	623
ν_{21}^*					1246	1246	1246	1246	1246	1246	623	623	623	623	623	623
ν_{22}^*						1246	1246	1246	1246	1246	624	623	623	623	623	623
ν_{23}^*							1246	1246	1246	1246	1246	623	623	623	623	623
ν_{24}^*								1246	1246	1246	1246	624	623	623	623	623
ν_{25}^*									1246	1246	1246	1246	623	623	623	623
ν_{26}^*										1246	1246	1246	624	623	623	623
ν_{27}^*											1246	1246	623	623	623	623
ν_{28}^*												1246	1246	624	623	623
ν_{29}^*													1246	1246	623	623
ν_{30}^*														1246	624	623
ν_{31}^*															1246	623
ν_{32}^*																624
$d(v)$	549	484	426	373	326	283	243	207	174	143	115	89	64	41	20	0
N_v	7	6	6	6	6	6	6	6	6	6	6	6	6	6	5	5

From a comparison of the lower r coordinates, it is easy to see that there exist $\mathbb{F}_2$-linear relations among $\{\mathbf{y}_i, \mathbf{y}_{i+n_2-n_1}, \mathbf{y}_{i-n_1}\}$. The Couture–L'Ecuyer dual lattice method gives explicit $\mathbb{F}_2$-linear relations without direct matrix computations, and it is applicable not only for Mersenne Twisters defined by (1) and (2) but also for general $\mathbb{F}_2$-linear generators.

7. Birthday spacings tests for non-successive output values

In this section, we report statistical tests for non-successive output values of MT19937. In particular, we conduct the birthday spacings test proposed by Marsaglia [22], which was further studied by Knuth [11] and L'Ecuyer and Simard [14]. We consider a similar technique proposed in [16, 12] for the detection of deviations of Deng and his co-authors' multiple recursive generators (e.g., [4]).

Following the notations of [14, 17], we introduce the testing procedure. We fix two positive integers, n and t, and generate n "independent" points $\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}$ in the t-dimensional hypercube $[0,1)^t$. For the hypercube, we partition it into d^t cubic boxes of equal size by dividing $[0,1)$ into d equal

segments. These boxes are numbered from 0 to $d^t - 1$ in lexicographic order, namely, the box with the lower left corner at $(i_0/d, \ldots, i_{t-1}/d)$ has the number $c = i_0 d^{t-1} + i_1 d^{t-2} + \cdots + i_{t-1}$. Let $I_1 \le I_2 \le \cdots \le I_n$ be the numbers of the boxes where these points have fallen, sorted by increasing order. Define the spacings $S_j := I_{j+1} - I_j$, for $j = 1, \ldots, n-1$. Let Y be the total number of collisions of these spacings, i.e., the number of values of $j \in \{1, \cdots, n-2\}$ such that $S_{(j+i)} = S_{(i)}$, where $S_{(1)}, \ldots, S_{(n-1)}$ are the spacings sorted by increasing order. We can view each points $\mathbf{u}_i$ as a "person" with a birthday I_i in a year having k days. We test the null hypothesis $\mathcal{H}_0$: the PRNG produces i.i.d. $U(0,1)$ random variables. If d^t is large and $\lambda = n^3/(4d^t)$ is not too large, Y is approximately a Poisson distribution with mean λ under $\mathcal{H}_0$ (see 3.3.2-28–30 in [11]). We generate independent N replications of Y, and add them. We compute the p-value by using the sum, which is approximately a Poisson distribution with mean $N\lambda$, under $\mathcal{H}_0$. As a rule of thumb, the error of approximation is negligible when $d^t \ge (4N\lambda)^4$(see [14]). Our experiments satisfy this rule of thumb. If $d = 2^v$, note that the t-dimensional output with v-bit accuracy is tested.

To extract non-successive output values, let us consider the t-dimensional output vectors constructed as

$$\mathbf{u}_i = (u_{(j_t+1)i+j_1}, \ldots, u_{(j_t+1)i+j_t}),$$

for $i = 0, \ldots, n-1$ with lags $I = \{j_1, \ldots, j_t\}$. In our experiments, we use the birthday spacings tests implemented in the TestU01 package [15], which is a software library for statistical tests for pseudorandom number generators.

First, we conduct experiments with the parameter set $(N, n, d, t) = (5, 20000000, 2^{21}, 3)$, which is just No. 12 of Crush in TestU01. Then, the three-dimensional output with 21-bit accuracy is tested. As expected, for the points using successive output values (i.e., $I = \{0, 1, 2\}$) by MT19937, the result appears to be good (see [15]). On th other hand, we construct the points with the lag based on $I = \{0, 396, 623\}$. The second row in Table 3 gives right p-values for five initial states, and all the p-values are $< 10^{-15}$. Thus, MT19937 with $I = \{0, 396, 623\}$ decisively fails the birthday spacings tests. This is probably because there exist low-weight minimal $\mathbb{F}_2$-linear relations with 21-bit accuracy in Section 6. It takes approximately eight minutes on an Intel Core i7-3770 3.90 GHz computer (with the gcc compiler with a `-O3` optimization flag on a Linux operating system) for each test.

Next, we conduct birthday spacings tests five times with the parameter set $(N, n, d, t) = (5, 15000000, 2^{12}, 5)$. Thus, the five-dimensional output with

12-bit accuracy is tested. The third row in Table 3 shows small deviations for the points with $I = \{0, 396, 623, 792, 1246\}$. It takes approximately 11 minutes for each test in the above environment. Furthermore, we focus on the five-term $\mathbb{F}_2$-linear relation (16). The last row of Table 3 shows similar deviations of the birthday spacings tests for $(N, n, d, t) = (5, 20000000, 2^{21}, 3)$ and $I = \{0, 792, 1246\}$.

Table 3: The p-values on the birthday spacings tests with selected lags I for MT19937.

	1st	2nd	3rd	4th	5th
$I = \{0, 396, 623\}$	1.7×10^{-16}	1.8×10^{-18}	3.1×10^{-21}	8.5×10^{-17}	1.4×10^{-21}
$I = \{0, 396, 623, 792, 1246\}$	4.8×10^{-5}	0.01	1.5×10^{-4}	1.1×10^{-4}	8.5×10^{-4}
$I = \{0, 792, 1246\}$	2.0×10^{-4}	3.0×10^{-7}	3.9×10^{-6}	9.2×10^{-5}	4.5×10^{-6}

8. Some variants of Mersenne Twister generators

We analyze other $\mathbb{F}_2$-linear generators whose periods are $2^{19937} - 1$ (i.e., $p = 19937$ and $w = 32$). First, we investigate the WELL generators [34], which are variants of Mersenne Twister and have almost optimal $k(v)$ and N_1. A key idea of the improvement is to construct a more complicated transition matrix $\mathbf{A}$ in (6) by using linear recurrences with a double loop, instead of that with a single loop (1) (see [36] for details). Panneton et al. [34] list the parameters of WELL generators WELL19937a, which has $\Delta = 4$, and WELL19937c, which has $\Delta = 0$ (i.e., maximally equidistributed) by adding the Matsumoto–Kurita tempering [24]. The author [7] also introduced more simplified temperings required to attain the maximal equidistribution. (We discovered a typo in Table 4 of [7]. The bitmask `4202000` should be corrected to `4202010`.) All of the WELL generators have $N_1 = 8585$ and $N_v > 9500$ $(2 \le v \le 32)$, so that we have no low-weight minimal $\mathbb{F}_2$-linear relations. This implies that we have no suitable lags for which birthday spacings tests are rejected in $(k(v) + 1)$-dimensional output values. In this respect, the WELL generators are much superior to MT19937.

As another improvement, the author [7] constructed a maximally equidistributed Mersenne Twister MEMT19937 by replacing the tempering in (7) and (8) with a more complicated output transformation $\mathbf{B}$, which consists

of a linear combination of some part of the state vector. However, the author recently noted the following drawbacks: (i) MEMT19937 is sometimes slower than WEL19937a on some recent platforms; (ii) MEMT19937 has a small value $N_{32} = 26$. Again, we search for a better parameter set by using the PIS method [8]. By trial-and-error, as well as in [7], we obtain a simple linear transformation:

$$\begin{aligned}
\mathbf{z} &\leftarrow \mathbf{m}_i, \\
\mathbf{z} &\leftarrow \mathbf{z} \oplus (\mathbf{m}_{i-603} \,\&\, \texttt{53c45278}), \\
\mathbf{z} &\leftarrow \mathbf{z} \oplus (\mathbf{z} \ll 8), \\
\mathbf{z} &\leftarrow \mathbf{z} \oplus (\mathbf{z} \ll 14), \\
\mathbf{z} &\leftarrow \mathbf{z} \oplus (\mathbf{z} \gg 18), \\
\mathbf{y}_i &\leftarrow \mathbf{z} \oplus (\mathbf{m}_{i-504} \,\&\, \texttt{fab7b141}),
\end{aligned}$$

where $\oplus$ denotes bitwise exclusive-or, & bitwise AND, $(\mathbf{z} \ll s_1)$ the s_1 bit left-shift, $(\mathbf{z} \gg s_2)$ the s_2 bit right-shift, and `53c45278` and `fab7b141` are hexadecimal notations. We replace the tempering (2) with the above, and we then obtain a maximally equidistributed generator. We name this MEMT19937-II. MEMT19937-II has $N_1 = 135$ and $N_v > 9000$ $(2 \le v \le 32)$, namely, N_v's significantly increase. This generator passes the Big Crush suits in the TestU01 statistical test library, with the exception of two linear complexity tests (the test number 80 and 81), and these rejections are common among $\mathbb{F}_2$-linear generators, such as the Mersenne Twister and WELL generators (see [15]). Now, MEMT19937-II is available on the author's homepage [9].

Here, we measure the speed to generate 10^9 32-bit unsigned integers on two different 64-bit CPUs: Intel Core i7-3770 3.90 GHz and AMD Phenom II X6 1045T 2.70 GHz. We use the gcc compiler with a `-O3` optimization flag on a Linux operating systems. In comparison, we also conduct experiments with MT19937ar, Shawn Cokus' other implementation MT19937ar-cok (both are obtained from [23]), and WEL19937a. Table 4 gives a summary of the CPU time (in seconds) and the total dimension defects Δ. MT19937ar-cok is the fastest, but the maximally equidistributed generator MEMT19937-II is comparable to MT19937ar on the two platforms.

Finally, we conduct birthday spacings tests for non-successive output values of MEMT19937-II. Table 5 gives a summary of birthday spacings tests with the same parameter sets for three- and five-dimensional non-successive

Table 4: CPU time (sec) taken to generate 10^9 pseudorandom numbers and total dimension defects Δ.

	Intel Core i7	AMD Phenom II	Δ
MT19937ar-cok	3.126	4.199	6750
MEMT19937-II	4.348	6.330	0
MT19937ar	4.771	6.106	6750
WELL19937a	4.953	6.678	4

outputs in Section 7. A simple improvement of $\mathbf{B}$ also increases N_v's, and deviations of tests are avoided.

Table 5: The p-values of birthday spacings tests five times for MEMT19937-II.

	1st	2nd	3rd	4th	5th
$I = \{0, 396, 623\}$	0.60	0.63	0.95	0.17	0.36
$I = \{0, 396, 623, 792, 1246\}$	0.33	0.57	0.17	0.10	0.03
$I = \{0, 792, 1246\}$	0.93	0.81	0.09	0.22	0.98

9. Conclusions

We have discussed the relationship between $\mathbb{F}_2$-linear relations and the Couture–L'Ecuyer dual lattices, and have proposed the new figure of merit N_v based on the minimum weight of $\mathbb{F}$-linear relations for most significant v bits in $(k(v)+1)$-dimensional output vectors. We presented an algorithm for computing N_v, and applied it to the Mersenne Twister MT19937. The results showed that MT19937 has low-weight $\mathbb{F}_2$-linear relations, and is rejected for birthday spacings tests with specific lags, and the reason appears to be the existence of such $\mathbb{F}_2$-linear relations. To avoid such phenomena, some improvements of Mersenne Twister generators were also discussed.

The above result of MT19937 will not affect most Monte Carlo simulations because real simulations are not synchronized with bad lag sets I. However, in general, when strange phenomena occur in simulations, and when these are due to the regularity of pseudorandom number generators, it is significantly difficult for experimenters to determine the reason for occurrence of

the strange phenomena. Thus, when designing pseudorandom number generators, it is important to perform assessments in as many situations as possible beforehand. In this respect, the Couture–L'Ecuyer lattices are powerful tools not only for computing $k(v)$ but also for detecting hidden structural defects of $\mathbb{F}_2$-linear generators.

Acknowledgments

This work was partially supported by JSPS Research Fellowships for Young Scientists, JSPS Grant-In-Aid #21654017, #23244002, and Global COE Program "The Research and Training Center for New Development in Mathematics" from MEXT, Japan.

References

[1] A. Compagner, The hierarchy of correlations in random binary sequences, Journal of Statistical Physics 63 (1991) 883–896. 10.1007/BF01029989.

[2] R. Couture, P. L'Ecuyer, Lattice computations for random numbers, Math. Comput. 69 (2000) 757–765.

[3] R. Couture, P. L'Ecuyer, S. Tezuka, On the distribution of k-dimensional vectors for simple and combined Tausworthe sequences, Math. Comput. 60 (1993) 749–761.

[4] L.P. Deng, D. Lin, Random number generation for the new century, The American Statistician 54 (2000) 145–150.

[5] M. Fushimi, S. Tezuka, The k-distribution of generalized feedback shift register pseudorandom numbers, Commun. ACM 26 (1983) 516–523.

[6] J. von zur Gathen, Hensel and Newton methods in valuation rings, Math. Comp. 42 (1984) 637–661.

[7] S. Harase, Maximally equidistributed pseudorandom number generators via linear output transformations, Math. Comput. Simul. 79 (2009) 1512–1519.

[8] S. Harase, An efficient lattice reduction method for $\mathbf{F}_2$-linear pseudorandom number generators using mulders and storjohann algorithm, Journal of Computational and Applied Mathematics 236 (2011) 141 – 149.

[9] S. Harase, 2013. http://www3.ocn.ne.jp/~harase/megenerators2.html.

[10] S. Harase, M. Matsumoto, M. Saito, Fast lattice reduction for $\mathbf{F}_2$-linear pseudorandom number generators, Math. Comput. 80 (2011) 395–407.

[11] D.E. Knuth, The Art of Computer Programming, Volume 2 (3rd ed.): Seminumerical Algorithms, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[12] P. L'Ecuyer, A. Ionut, R. Simard, On the lattice structure of a special class of multiple recursive random number generators, 2012. Preprint.

[13] P. L'Ecuyer, F. Panneton, $\mathbb{F}_2$-linear random number generators, in: C. Alexopoulos, D. Goldsman, J.R. Wilson (Eds.), Advancing the Frontiers of Simulation: A Festschrift in Honor of George Samuel Fishman, Springer-Verlag, 2009, pp. 169–193.

[14] P. L'Ecuyer, R. Simard, On the performance of birthday spacings tests with certain families of random number generators, Math. Comput. Simulation 55 (2001) 131–137. The Second IMACS Seminar on Monte Carlo Methods (Varna, 1999).

[15] P. L'Ecuyer, R. Simard, TestU01: a C library for empirical testing of random number generators, ACM Trans. Math. Software 33 (2007) Art. 22, 40.

[16] P. L'Ecuyer, R. Touzin, On the Deng-Lin random number generators and related methods, Statistics and Computing 14 (2004) 5–9.

[17] C. Lemieux, Monte Carlo and quasi-Monte Carlo sampling, Springer Series in Statistics, Springer, New York, 2009.

[18] A.K. Lenstra, Factoring multivariate polynomials over finite fields, Journal of Computer and System Sciences 30 (1985) 235 – 248.

[19] J.H. Lindholm, An analysis of the pseudo-randomness properties of subsequencesof long m-sequences, IEEE Trans. Inform. Theory IT-14 (1968) 569–576.

[20] K. Mahler, An Analogue to Minkowski's Geometry of Numbers in a Field of Series, The Annals of Mathematics 42 (1941) 488–522.

[21] K. Mahler, On a theorem in the geometry of numbers in a space of Laurent series, Journal of Number Theory 17 (1983) 403 – 416.

[22] G. Marsaglia, A current view of random number generators, in: Computer Science and Statistics, Sixteenth Symposium on the Interface, Elsevier Science Publisher, North-Holland, Amsterdam, The Netherlands, 1985, pp. 3–10.

[23] M. Matsumoto, Mersenne Twister Homepage, since 1997/10. `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html`.

[24] M. Matsumoto, Y. Kurita, Twisted GFSR generators II, ACM Trans. Model. Comput. Simul. 4 (1994) 254–266.

[25] M. Matsumoto, Y. Kurita, Strong deviations from randomness in m-sequences based on trinomials, ACM Trans. Model. Comput. Simul. 6 (1996) 99–106.

[26] M. Matsumoto, T. Nishimura, Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator, ACM Trans. Model. Comput. Simul. 8 (1998) 3–30.

[27] M. Matsumoto, T. Nishimura, A nonempirical test on the weight of pseudorandom number generators, in: Monte Carlo and quasi-Monte Carlo methods, 2000 (Hong Kong), Springer, Berlin, 2002, pp. 381–395.

[28] M. Matsumoto, M. Saito, H. Haramoto, T. Nishimura, Pseudorandom Number Generation: Impossibility and Compromise, J. Univer. Comput. Sci. 12 (2006) 672–690.

[29] T. Mulders, A. Storjohann, On lattice reduction for polynomial matrices, J. Symb. Comput. 35 (2003) 377–401.

[30] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods. SIAM CBMS-NSF Reginal Conference Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992.

[31] H. Niederreiter, Factorization of polynomials and some linear-algebra problems over finite fields, Linear Algebra Appl. 192 (1993) 301–328. Computational linear algebra in algebraic and related problems (Essen, 1992).

[32] H. Niederreiter, The multiple-recursive matrix method for pseudorandom number generation, Finite Fields Appl. 1 (1995) 3–30.

[33] F. Panneton, Construction dénsembles de points basée sur des récurrences linéaires dans un corps fini de caractéristique 2 pour la simulation Monte Carlo et líntégration quasi-Monte Carlo, Ph.D. thesis, Département dínformatique et de recherche opérationnelle, Université de Montréal, Canada, 2004.

[34] F. Panneton, P. L'Ecuyer, M. Matsumoto, Improved long-period generators based on linear recurrences modulo 2, ACM Trans. Math. Softw. 32 (2006) 1–16.

[35] R Core Team, R: A Language and Environment for Statistical Computing, R Foundation for Statistical Computing, Vienna, Austria, 2012. ISBN 3-900051-07-0.

[36] M. Saito, M. Matsumoto, A PRNG specialized in double precision floating point numbers using an affine transition, in: Monte Carlo and quasi-Monte Carlo methods 2008, Springer, Berlin, 2009, pp. 589–602.

[37] W.M. Schmidt, Construction and estimation of bases in function fields, J. Number Theory 39 (1991) 181 – 224.

[38] S. Tezuka, The k-dimensional distribution of combined GFSR sequences, Math. Comput. 62 (1994) 809–817.

[39] J.P.R. Tootill, W.D. Robinson, D.J. Eagle, An Asymptotically Random Tausworthe Sequence, J. ACM 20 (1973) 469–481.

[40] A. Vardy, The intractability of computing the minimum distance of a code, IEEE Trans. Inform. Theory 43 (1997) 1757–1766.

[41] D.K. Wang, A. Compagner, On the use of reducible polynomials as random number generators, Math. Comp. 60 (1993) 363–374.